What Is Claimed Is:

1. A method for performing a cryptographic operation that comprises transforming digital information, the method comprising:

providing digital information;

providing a digital operator having a component selected from a large set of elements;

expanding the component into a plurality of factors, each factor having a low Hamming weight; and

transforming the digital information using the digital operator.

2. The method of claim 1, wherein the cryptographic operation is selected from the group consisting of key generation, encryption, decryption, creation of a digital signature, verification of a digital signature, creation of a digital certificate, authentication of a digital certificate, identification, pseudorandom number generation and computation of a hash function.

3. The method of claim 1, wherein the Hamming weight is less than about 30.

4. The method of claim 1, wherein the Hamming weight is less than about 20.

5. The method of claim 1, wherein the Hamming weight is less than about 15.

6. The method of claim 1, wherein the step of transforming comprises computing multiples, said method further comprising:

selecting a ring R;

selecting an R-module M;

selecting two or more subsets R_1, R_2, ... , R_k of R with the property that r_1 is an element in R_1, r_2 is an element in R_2, ... and r_k is an element in R_k;

computing r*m, where r is in R and m is in M, by expanding r as $r_1*r_2*...r_k$, where k is an integer and computing the quantity $r_1*(r_2*(...(r_k*m)$.

7. The method of claim 6, wherein the cryptographic operation is selected from the group consisting of key generation, encryption, decryption, creation of a digital signature, verification of a digital signature, creation of a digital certificate, authentication of a digital certificate, identification, pseudorandom number generation and computation of a hash function.

8. The method of claim 6, wherein each r_k has a Hamming weight that is less than about 15.

9. The method of claim 6, wherein each r_k has a Hamming weight that is less than about 10.

10. The method of claim 6, wherein the subset R_i is a subset of R consisting of elements of the form

$$a_1 t^{e(1)} + a_2 t^{e(2)} + \ldots + a_n t^{e(n)},$$

wherein n is an integer.

11. The method of claim 10, wherein each of the elements $a_1, \ldots, a_n$ are chosen from the set {0,1}.

12. The method of claim 10, wherein each of the elements $a_1, \ldots, a_n$ are chosen from the set {-1,0,1}.

13. The method of claim 6, wherein the subset R_i is a subset of R consisting of polynomials in elements of $t_1, \ldots, t_k$ of R having coefficients $a_1, \ldots, a_k$ taken from a subset A of R where k is an integer.

14. The method of claim 13, wherein each of the coefficients $a_1, \ldots, a_k$ is chosen from the set {0,1}.

15. The method of claim 13, wherein each of the coefficients $a_1, \ldots, a_k$ is chosen from the set {-1,0,1}.

16. The method of claim 6, wherein the ring R is the ring of integers, the R-module M is a group of nonzero elements in the field $GF(p^m)$ with p^m elements, and wherein the subsets $R_1, \ldots, R_k$ consist of integers of the form

$$a_1 p^{e(1)} + a_2 p^{e(2)} + \ldots + a_n p^{e(n)},$$

wherein n is an integer that is less than m and wherein $a_1, \ldots, a_n$ are elements of the set {0,1}.

17. The method of claim 6, wherein the ring R is the ring of integers, the R-module M is a group of nonzero elements in the field $GF(p^m)$ with p^m elements, and wherein the subsets $R_1, \ldots, R_k$ consist of integers of the form

$$a_1 p^{e(1)} + a_2 p^{e(2)} + \ldots + a_n p^{e(n)},$$

wherein n is an integer that is less than m and wherein $a_1, \ldots, a_n$ are elements of a small set of integers A.

18. The method of claim 6, wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q).

19. The method of claim 6, wherein the module M is a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q).

20. The method of claim 10, wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q) of characteristic p, wherein the module M is a group of points E(GF(q)) and wherein the element t is a p-power Frobenius map.

21. The method of claim 10, wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q) of characteristic p and the module M is a group of points E(GF(q)) and wherein the element t is a point halving map.

22. The method of claim 6, wherein the ring R is a ring of polynomials modulo an ideal A[X]/I, wherein A is a ring and I is an ideal of A[X], and wherein the subsets $R_1,\ldots,R_k$ are sets of polynomials with few nonzero terms.

23. The method of claim 22, wherein the ideal I is the ideal generated by the polynomial X^N-1.

24. The method of claim 22, wherein the ring A is a finite ring $\mathbf{Z}/q\mathbf{Z}$ of integers modulo q, wherein q is a positive integer.

25. The method of claim 10, wherein the ring R is a ring of polynomials modulo an ideal A[X]/I, wherein A is a ring and I is an ideal of A[X], and wherein the element t is the polynomial X in R.

26. The method of claim 25, wherein the ideal I is the ideal generated by the polynomial X^N-1.

27. The method of claim 25, wherein the ring A is a finite ring $\mathbf{Z}/q\mathbf{Z}$ of integers modulo q, wherein q is a positive integer.

28. A computer readable medium containing instructions for a method for performing a cryptographic operation that comprises transforming digital information, the method comprising:

providing digital information;

providing a digital operator having a component selected from a large set of elements;

expanding the component into a plurality of factors, each factor having a low Hamming weight; and

transforming the digital information using the digital operator.

29. The computer readable medium of claim 28, containing instructions for a method further comprising:

selecting a ring R;

selecting an R-module M;

selecting two or more subsets R_1, R_2, ... , R_k of R with the property that r_1 is an element in R_1, r_2 is an element in R_2, ... and r_k is an element in R_k;

computing r*m, where r is in R and m is in M, by expanding r as $r_1*r_2*...r_k$, where k is an integer and computing the quantity $r_1*(r_2*(...(r_k*m)$.

30. The computer readable medium of claim 29, containing instructions for a method wherein the subset R_i is a subset of R consisting of elements of the form

$$a_1t^{e(1)} + a_2t^{e(2)} + ... + a_nt^{e(n)},$$

wherein n is an integer.

31. The computer readable medium of claim 29, containing instructions for a method wherein the subset R_i is a subset of R consisting of polynomials in elements of t_1, ..., t_k of R having coefficients a_1, ..., a_k taken from a subset A of R where k is an integer.

32. The computer readable medium of claim 29, containing instructions for a method wherein the ring R is the ring of integers, the R-module M is a group of nonzero elements in the field $GF(p^m)$ with p^m elements, and wherein the subsets R_1, ..., R_k consist of integers of the form

$$a_1p^{e(1)} + a_2p^{e(2)} + ... + a_np^{e(n)},$$

wherein n is an integer that is less than m and wherein a_1, ..., a_n are elements of the set {0,1}.

33. The computer readable medium of claim 29, containing instructions for a method wherein the ring R is the ring of integers, the R-module M is a group of nonzero elements in the field $GF(p^m)$ with p^m elements, and wherein the subsets R_1, ..., R_k consist of integers of the form

$$a_1p^{e(1)} + a_2p^{e(2)} + ... + a_np^{e(n)},$$

wherein n is an integer that is less than m and wherein a_1, ..., a_n are elements of a small set of integers A.

34. The computer readable medium of claim 29, containing instructions for a method wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q).

35. The computer readable medium of claim 29, containing instructions for a method wherein the module M is a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q).

36. The computer readable medium of claim 30, containing instructions for a method wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q) of characteristic p, wherein the module M is a group of points E(GF(q)) and wherein the element t is a p-power Frobenius map.

37. The computer readable medium of claim 30, containing instructions for a method wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q) of characteristic p and the module M is a group of points E(GF(q)) and wherein the element t is a point halving map.

38. The computer readable medium of claim 29, containing instructions for a method wherein the ring R is the ring of polynomials modulo an ideal A[X]/I, wherein A is a ring and I is an ideal of A[X], and wherein the subsets R_1,...,R_k are sets of polynomials with few nonzero terms.

39. The computer readable medium of claim 30, containing instructions for a method wherein the ring R is the ring of polynomials modulo an ideal A[X]/I, wherein A is a ring and I is an ideal of A[X], and wherein the element t is the polynomial X in R.